



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/465,629	12/17/1999	LEWIS T. DONZIS	NORT-0030-US	9110

7590 03/30/2004

DAN C HU
TROP PRUNER HU & MILES PC
8554 KATY FREEWAY
SUITE 100
HOUSTON, TX 77024

EXAMINER

WU, ALLEN S

ART UNIT PAPER NUMBER

2135

DATE MAILED: 03/30/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

7

Office Action Summary

Application No.

09/465,629

Applicant(s)

DONZIS ET AL.

Examiner

Allen S. Wu

Art Unit

2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 1/23/04
- 2a) ☒ This action is FINAL. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-4, 8-15, 17-21, 24-28, and 35-36 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-4, 8-15, 17-21, 24-28, and 35-36 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 17 December 1999 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

- ju* 2. Claims 1-4, 8-15, ~~16~~⁷-21, ~~24~~²⁴28, and 35-36 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nessel et al, US Patent 6,055,236, in view of Maughan et al.

As per claim 1, Nessel et al discloses a method of routing (Abstract) a data unit (data packets, col 7 ln 8-33) targeted to one of a plurality of entities in a network (multiple network devices, col 7 ln 8-33), comprising: receiving the data unit (IP packet arrives at the router, col 32 ln 50-64), the data unit including security information (AH or ESP IPsec packet, col 32 ln 50-64; locally unique security values, col 27 ln 36-50) and address information (network address for first network device, col 27 ln 36-50; global IP address placed in service request packet, col 35 ln 64-67 and col 36 ln 1-12).

Nessel et al further discloses the information including Internet Security Association and Key Management Protocol information (Internet Security Association and Key Exchange Protocol to establish security association col 25 ln 1-25; ISAKMP is a standard protocol that is well known in the art. When ISAKMP is being used to establish a Security Association, its header is placed

with the IP packet. Therefore, the data unit containing IP address information inherently contains ISAKMP information in the teachings of Nessett et al).

Nessett et al further discloses translating the address information to an address of a target network entity based on the security information (using SPI's to determine a local IP address, col 32 ln 50-64). Nessett does not explicitly teach translating the address the ISAKMP information. Maughan et al discloses Internet Security Association and Key Management Protocol with a header including initiator and responder cookies (page 21), such that the initiator and responder cookies correspond to the SPI value (page 28). The initiator and responder cookies correspond to information identifying the initiator and responder devices. The Security Parameters Index field of Encapsulating Security Payload information also identifies the network entities for a Security Association. Both the cookies and the Security Payload Index field serve as some kind of identification of network entities requesting the Security Association and are stored as digital data in the headers of the corresponding protocol. It would have been obvious to one of ordinary skill at the time of the applicant's invention to combine the teachings of Maughan et al within the system of Nessett et al because it would have provided another security protocol for identifying and translating network addresses information to a local network entity.

As per claim 2, Nessett et al discloses the address information, in the data unit, including a common address associated with the plurality of network entities

(global IP address placed in service request packet, col 35 ln 64-67 and col 36 ln 1-12), and each network entity is assigned a unique network address (local IP address, col 32, ln 50-64), and wherein translating the address information includes translating the common address to one of the unique network addresses (using SPI's to determine a local IP address, col 32 ln 50-64; translate external network address to internal network address, col 8 ln 30-40).

As per claim 3, Nessett et al discloses receiving an Internet Protocol packet (IPsec header protocols are added to a IP packet, col 21 ln 43-47).

As per claim 4, Nessett et al discloses translating an Internet Protocol destination address (determine local IP address of a destination network device, col 32 ln 50-64).

As per claims 8, 35, and 36, Nessett et al discloses translating the address based on ISAKMP, as described above (see claim 1). Maughan et al discloses Internet Security Association and Key Management Protocol with a header including initiator and responder cookies (page 21 and page 28). The initiator and responder cookies correspond to information identifying the initiator and responder devices. The Security Parameters Index field of Encapsulating Security Payload information also identifies the network entities for a Security Association. Both the cookies and the Security Payload Index field serve as

some kind of identification of network entities requesting the Security Association and are stored as digital data in the headers of the corresponding protocol. It would have been obvious to one of ordinary skill at the time of the applicant's invention to combine the teachings of Maughan et al within the system of Nessett et al because it would have provided another security protocol for identifying and translating network addresses information to a local network entity.

In further regards to claim 36, Nessett et al further discloses the information including Internet Security Association and Key Management Protocol information (Internet Security Association and Key Exchange Protocol to establish security association col 25 ln 1-25; ISAKMP is a standard protocol that is well known in the art. When ISAKMP is being used to establish a Security Association, its header is placed with the IP packet. Therefore, the data unit containing IP address information inherently contains ISAKMP information in the teachings of Nessett et al). Furthermore, ISAKMP header is well known in the art to contain initiator and responder cookies (see Maughan et al page 21).

As per claim 9, Nessett et al discloses creating one or more address translation tables (SPI-to-internal-network address table, col 27 ln 51-67 and col 28 ln 1-34) used in the translation of address information (col 27 51-67 and col 28 ln 1-34), the one or more address translation tables each containing the address of at least one of the network entities and ISAKMP information associated with the at least one network entity (local IP address for first network

device is stored with the one or more locally unique SPI values in a table, col 27 51-67, col 28 ln 1-34, and col 32 ln 11-40).

As per claim 10, Nessett et al discloses matching the ISAKMP information in the data unit with the information in the one or more address translation tables (table is used to maintain a mapping between a network device and a locally unique SPI, col 28 ln 1-34).

As per claim 11, Nessett et al discloses a router for use in a network having one or more entities (col 7 ln 8-33), the router comprising: an interface adapted to receive a data unit (col 7 ln 8-33); In order for a router to receive and process IP packets, an interface in the router is necessary. Therefore, an interface adapted to receive a data unit is inherent to the invention of Nessett et al)

Nessett et al further discloses the information including Internet Security Association and Key Management Protocol information (Internet Security Association and Key Exchange Protocol to establish security association col 25 ln 1-25; ISAKMP is a standard protocol that is well known in the art. When ISAKMP is being used to establish a Security Association, its header is placed with the IP packet. Therefore, the data unit containing IP address information inherently contains ISAKMP information in the teachings of Nessett et al); and a translator adapted to generate an identifier of a network entity that the data unit is

targeted for (Network Address Translation router, col 8 ln 30-52) based on the security information (using SPI's to determine a local IP address, col 32 ln 50-64). Nessel et al does not explicitly teach translating the address based ISAKMP information. Maughan et al discloses Internet Security Association and Key Management Protocol with a header including initiator and responder cookies (page 21), such that the initiator and responder cookies correspond to the SPI value (page 28). The initiator and responder cookies correspond to information identifying the initiator and responder devices. The Security Parameters Index field of Encapsulating Security Payload information also identifies the network entities for a Security Association. Both the cookies and the Security Payload Index field serve as some kind of identification of network entities requesting the Security Association and are stored as digital data in the headers of the corresponding protocol. It would have been obvious to one of ordinary skill at the time of the applicant's invention to combine the teachings of Maughan et al within the system of Nessel et al because it would have provided another security protocol for identifying and translating network addresses information to a local network entity.

As per claim 12, Nessel et al discloses a many-to-one network address translator (Network address translator router, col 8 ln 30-40; It is noted that Nessel et al does not explicitly state a many-to-one network address translator. The translator disclosed by Nessel et al translates local IP addresses of network

entities to one common, external, address. Therefore, the translator of Nessett et al is inherently a many-to-one address translator).

As per claim 13, Nessett et al discloses the data unit further contains an address associated with the router (external common network address, col 7 ln 8-33; The common address being associated with the router is to be inherent to the invention of Nessett et al. The global external IP address needs to be associated with a router in order for other external networks, such as the Internet, to communicate with the internal network through the router)

As per claim 14, Nessett et al discloses the translator being adapted to further replace the address with the identifier of the target network entity (map destination port to internal IP address, col 16 ln 13-25; using SPI's to determine a local IP address, col 32 ln 50-64).

As per claim 15, Nessett et al discloses translating an Internet Protocol destination address (determine local IP address of a destination network device, col 32 ln 50-64).

As per claim 17, Nessett et al discloses the data unit containing initiator and responder cookies in an Internet Security Association and Key Management Protocol (here in after referred to as ISAKMP) header (using ISAMKP for

Security Association negotiation, col 25 ln 16-25; Nessett et al does not explicitly teach initiator and responder cookies in the data unit. ISAKMP is a standard protocol that is well known in the art. When ISAKMP is being used to establish a Security Association, its header is placed with the IP packet. The header information includes initiator and responder cookies. Therefore, the data unit containing initiator and responder cookies in an ISAKMP is to be inherent to the teachings of Nessett et al.)

As per claim 18, Nessett et al discloses a storage medium storing one or more tables containing routing information accessible by the translator (SPI-to-internal-network address table, col 27 ln 51-67 and col 28 ln 1-34).

As per claim 19, Nessett et al discloses the routing information includes security information and a corresponding identifier of a network entity (local IP address for first network device is stored with the one or more locally unique SPI values in a table, col 27 51-67 and col 28 ln 1-34).

As per claim 20, Nessett et al discloses an article including one or more machine-readable storage media containing instructions for routing (col 8 ln 8-19) a data unit targeted to an entity on a network (col 7 ln 8-33), the instructions when executed causing a system to: receive the data unit (IP packet arrives at the router, col 32 ln 50-64). Nessett et al further discloses the information

including Internet Security Association and Key Management Protocol information (Internet Security Association and Key Exchange Protocol to establish security association col 25 ln 1-25; ISAKMP is a standard protocol that is well known in the art. When ISAKMP is being used to establish a Security Association, its header is placed with the IP packet. Therefore, the data unit containing IP address information inherently contains ISAKMP information in the teachings of Nessett et al).

Nessett et al further discloses determining an address of the network entity based on the security information (using SPI's to determine a local IP address, col 32 ln 50-64).

Nessett does not explicitly teach translating the address the ISAKMP information. Maughan et al discloses Internet Security Association and Key Management Protocol with a header including initiator and responder cookies (page 21), such that the initiator and responder cookies correspond to the SPI value (page 28). The initiator and responder cookies correspond to information identifying the initiator and responder devices. The Security Parameters Index field of Encapsulating Security Payload information also identifies the network entities for a Security Association. Both the cookies and the Security Payload Index field serve as some kind of identification of network entities requesting the Security Association and are stored as digital data in the headers of the corresponding protocol. It would have been obvious to one of ordinary skill at the time of the applicant's invention to combine the teachings of Maughan et al within

the system of Nessett et al because it would have provided another security protocol for identifying and translating network addresses information to a local network entity.

As per claim 21, Nessett et al discloses translating an address in the data unit to the address of the network entity based on the ISAKMP (using SPI's to determine a local IP address, col 32 ln 50-64; translating an external network address to an internal network address for incoming traffic, col 8 ln 30-40l).

As per claim 24, Nessett et al discloses accessing an address translation table to match the ISAKMP information in the data unit to information in the address translation table (table is used to maintain a mapping between a network device and a locally unique SPI, col 28 ln 1-34 and col 43 ln 11-49; IKE SPI is based on initiator and responder cookies).

As per claim 25, Nessett et al discloses matching address and ISAKMP (IKE SPI, col 32 ln 11-49) information in the data unit with address and ISAKMP information in the address translation table (SPI-to-internal network address table, col 27 ln 36-67; table is used to maintain a mapping between a network device and a locally unique SPI, col 28 ln 1-34).

As per claim 26, Nessett et al discloses a data signal embodied in a carrier wave (electric signal, col 8 ln 8-19) comprising one or more code segments containing instructions (data bits, col 8 ln 8-19) for routing a data unit to one of a plurality of network entities (col 7 ln 8-33), the instructions when executed causing a system to: receive the data unit having security information and a destination address (IP packet arrives at the router, col 32 ln 50-64); access one or more translation tables (SPI-to-internal-network address table, col 27 ln 51-67 and col 28 ln 1-34) each containing security information and an address of a network entity (local IP address for first network device is stored with the one or more locally unique SPI values in a table, col 27 51-67 and col 28 ln 1-34).

Nessett et al further discloses the security information including Internet Security Association and Key Management Protocol information (Internet Security Association and Key Exchange Protocol to establish security association col 25 ln 1-25; ISAKMP is a standard protocol that is well known in the art. When ISAKMP is being used to establish a Security Association, its header is placed with the IP packet. Therefore, the data unit containing IP address information inherently contains ISAKMP information in the teachings of Nessett et al).

Nessett et al further discloses translating the address information to an address of a target network entity based on the security information (using SPI's to determine a local IP address, col 32 ln 50-64). Nessett does not explicitly teach translating the address based on ISAKMP information. Maughan et al

discloses Internet Security Association and Key Management Protocol with a header including initiator and responder cookies (page 21), such that the initiator and responder cookies correspond to the SPI value (page 28). The initiator and responder cookies correspond to information identifying the initiator and responder devices. The Security Parameters Index field of Encapsulating Security Payload information also identifies the network entities for a Security Association. Both the cookies and the Security Payload Index field serve as some kind of identification of network entities requesting the Security Association and are stored as digital data in the headers of the corresponding protocol. It would have been obvious to one of ordinary skill at the time of the applicant's invention to combine the teachings of Maughan et al within the system of Nessett et al because it would have provided another security protocol for identifying and translating network addresses information to a local network entity.

As per claim 27, Nessett et al discloses a data unit containing a first destination address (external network address, col 8 ln 30-40) and the network entity having a second address (internal network address, col 8 ln 30-40), the data structure (IP packet col 32 ln 50-64) comprising the first destination address (external network address, col 8 ln 30-40), the second address (internal network address, col 8 ln 30-40), and Internet Security Association and Key Management Protocol (Security Parameter Index, col 21 ln 57-67, see claim 26 above) useable by the system to match the first destination address to the second address based

on the ISAKMP information (using SPI's to determine a local IP address, col 32 In 50-64, see claim 6 above).

As per claim 28, Nessett et al discloses a communications network (network system, col 7 In 8-33, comprising: a first network including a plurality of entities and a router (network devices and router, col 7 In 8-33), the router including a network address translator (network address translation router, col 8 In 39-40) and a node capable of communicating data units with entities in the first network (internet or intranet, col 7 In 34-49), each data unit including security information (AH or ESP IPsec packet, col 32 In 50-64; locally unique security values, col 27 In 36-50),

Nessett et al further discloses the information including Internet Security Association and Key Management Protocol information (Internet Security Association and Key Exchange Protocol to establish security association col 25 In 1-25; ISAKMP is a standard protocol that is well known in the art. When ISAKMP is being used to establish a Security Association, its header is placed with the IP packet. Therefore, the data unit containing IP address information inherently contains ISAKMP information in the teachings of Nessett et al).

Nessett et al further discloses the network address translator adapted to convert a destination address in a received data unit from the node to an address of one of the entities (translates an external network address to an internal network address, col 8 In 30-40) based on the security information in the

received data unit (using SPI's to determine a local IP address, col 32 ln 50-64).

Nessett does not explicitly teach translating the address the ISAKMP information.

Maughan et al discloses Internet Security Association and Key Management Protocol with a header including initiator and responder cookies (page 21), such that the initiator and responder cookies correspond to the SPI value (page 28).

The initiator and responder cookies correspond to information identifying the initiator and responder devices. The Security Parameters Index field of Encapsulating Security Payload information also identifies the network entities for a Security Association. Both the cookies and the Security Payload Index field serve as some kind of identification of network entities requesting the Security Association and are stored as digital data in the headers of the corresponding protocol. It would have been obvious to one of ordinary skill at the time of the applicant's invention to combine the teachings of Maughan et al within the system of Nessett et al because it would have provided another security protocol for identifying and translating network addresses information to a local network entity.

Response to Arguments

3. Objection to the title (see Remarks, page 8 paragraph 2) has been withdrawn.
4. Applicant's arguments filed 19 January 2004 have been fully considered but they are not persuasive.

In regards to applicant's remarks to the obviousness rejection of dependent claim 8 (see page 8 paragraph 5), applicant states that "Maughan does not teach or

suggest a modification of Nessett to achieve the translating of address information in a received data unit to an address of a target network entity based on ISAKMP information.” However, Nessett mentions ISAKMP as an example of the “many standards [that] have been proposed for protocols that establish SAs” (see col 25 ln 1-15). Nessett discloses that other embodiments with different Internet security protocols may exist (“other network devices, protocols, security values and secure connections could also be used”, col 32 ln 19-26).

Furthermore, the IKE protocol, as described by Nessett et al, is well known in the art to be an implementation of the ISAKMP framework. In regard to applicant’s remark that “Nessett recognizes the existence of ISAKMP, Nessett does not provide any teaching that address translation can be based on ISAKMP information carried in a data packet” and that “this is a significant indication that Nessett does not provide any suggestion or motivation to modify its teachings to perform address translation based ISAKMP information.” Nessett et al uses a unique security values to assign addresses (see col 32 ln 50-64), more specifically the IKE SPI value (see col 32 ln 11-27). Nessett et al further discusses that other security protocols may be used (col 32 ln 23-26). Even though, Nessett et al does not discuss an embodiment specifically geared towards ISAKMP protocols, he suggests that it ISAKMP be used as another security protocol. Furthermore, Nessett et al describes an embodiment using IKE protocol (col 32 ln 11-49), which is an implementation of the ISAKMP

framework. Therefore, Nessett et al does provide suggestion to modify its teachings to perform address translation based on other security protocols.

In further response to applicant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988) and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, Maughan et al describes security information that can be substituted directly into the teachings of Nessett et al, to result in address translation being based on ISAKMP information, and is not relied upon to teach address translation. Nessett et al already establishes that address translation can be done by security values, (col 27 ln 42-45), wherein the security values can be the IKE SPI value (col 32 ln 19-26), or other security protocols (col 3 ln 53-65), but is silent on the details involved with the IKE SPI values. Maughan et al discloses initiator and responder cookies in the ISAKMP protocol used for identification purposes (see page 20-21, ISAKMP header format) and that "the initiator and responder cookie pair from the ISAKMP header is the ISAKMP SPI (page 28, third bullet). IKE is well known in the art to be an implementation of the ISAKMP framework, which uses ISAKMP headers and payloads. Therefore, the IKE SPI value is also considered the initiator and responder cookies of ISAKMP,

in view of Maughan et al. Therefore, the examiner respectfully submits that Nessett et al suggests a means of using ISAKMP information, as disclosed in detail by Maughan et al, to perform address translation. Furthermore, Nessett et al recognizes different security measures in Internet Security Protocol (hereinafter Ipsec, col 21 ln 1-7) and the difficulties of implementing "NAT routers" with Ipsec (col 25 ln 54-64). Therefore, one of ordinary skill in the art at the time of the applicant's invention would have been motivated to route information using ISAKMP information so as to extend the network addressing to a variety of Internet security protocols. Furthermore, ISAKMP is a "standard [that] have been proposed for protocols that establish SAs" (see Nessett et al, col 25 ln 1-3). ISAKMP will be used more frequently, as most protocols will adapt to the standard, so that a need arises in translating addresses under the ISAKMP protocol.

Conclusion

5. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

Art Unit: 2135


the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Allen S. Wu whose telephone number is 703-305-0708. The examiner can normally be reached on Monday-Friday 9am-5pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 703-305-4393. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Allen Wu
Patent Examiner
Art Unit 2135



ALLEN WU
PATENT EXAMINER
TECHNOLOGY CENTER 2100